



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/053,421 | 01/16/2002 | Misao Kimura | FUJH 19.343 | 4291 |

26304 7590 11/15/2005

KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER

HAST, NATHAN D

ART UNIT PAPER NUMBER

2136

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|--------------------------------------|--------------------------------------|--|
| Office Action Summary | Application No. 10/053,421 | Applicant(s) KIMURA, MISAO | |
| | Examiner Nathan D. Hast | Art Unit 2136 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 January 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☒ Claim(s) 9 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 January 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>1</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Acknowledgement of Papers

1. This office action is in regard to all papers received as of 16 January 2002.

Information Disclosure Statement

2. An Information Disclosure Statement was received. The IDS disclosed three U.S. Patents all of which were reviewed. A signed and dated copy of this document is enclosed with the office action for your records.

Priority

3. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).
4. The certified copy has been filed in parent Application No. 10/053421, filed on 16 January 2002. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Objections

5. Claim 9 is objected to because of the following informalities: on the last line of the claim there is an error, which is believed to be typographical in nature ("de4yption", interpreted as "decryption"). Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claim 1 through 16 are rejected under 35 U.S.C. 102(b) as being anticipated by PGP Freeware version 6.5 (PGP), released in 1999, as described by the software's accompanying documentation "PGP Freeware for Windows 95, Windows 98, and Windows NT: User's Guide (version 6.5)", "Configuring Checkpoint VPN-1 for use with PGP VPN Client (PGP version 6.5.1 and Checkpoint VPN-1 version 4)", and "Introduction to Cryptography (PGP version 6.5.1)"; henceforth referred to as "User Guide", "Checkpoint", and "Intro" respectively.

8. As per claim 1, PGP anticipates, a communication network system having a central management device and a plurality of local area network systems, said central management device and said plurality of local area network systems being connected to each other, each of the plurality of local area network systems having a router and a terminal which are connected to each other via a local area network,

said central management device comprising:

a management database (User Guide: page 228, definition "public keyring") for storing at least one common (User Guide: page 229, definition "session key") key, each public (asymmetric) key assigned to each router and a public (asymmetric) key assigned to the central management device (User Guide: page 230, definition "trusted introducer"); and

a central-side encryption unit (Intro: page 5, second paragraph and Figure 1-3) for encrypting the common key by using each public key assigned to each router, and sending the encrypted common key to each router;

said router comprising:

a first router-side decryption unit (Intro: page 5, second paragraph and Figure 1-3) for decrypting the encrypted common key sent from said center-side encryption unit by using a secret key of the router;

a storage unit (User Guide: page 15, "System Requirements" section) for storing the common key after decryption by said first router-side decryption unit; and

a router-side encryption unit for encrypting communication data (Intro: page 6, "How PGP Works" section and Figure 1-4) to be sent from a first source terminal in a local area network system of the router to a first destination terminal in another local area network system, or communication data to be sent from the router to the central management device, by using the common key stored in said storage unit, and sending the encrypted communication data to another local area network or the central management device.

9. As per claim 2, PGP anticipates, the communication network system according to claim 1, wherein

said central-side encryption unit encrypts (Intro: page 5, second paragraph and Figure 1-3) the public keys and sends said encrypted public keys to each router (User Guide: page 230, definition "trusted introducer"),

said first router-side decryption unit (Intro: page 5, second paragraph and Figure 1-3) decrypts the encrypted public keys sent from the central-side encryption unit by using the secret key of the router,

said storage unit (User Guide: page 15, "System Requirements" section) stores the public keys after decryption by said first router-side decryption unit, and

said router-side encryption unit (Intro: page 6, "How PGP Works" section and Figure 1-4) selects the public key for a router of another local area network system or the central management device to be a destination from the public keys stored in the storage unit, encrypts the common key by using the selected public key, and sends the encrypted common key to another local area network or the central management device together with the encrypted communication data.

10. As per claim 3, PGP anticipates, the communication network system according to claim 1, wherein

said management database further stores secret concealment terminal data indicating a combination of one terminal in one of the plurality of local area network systems and another terminal (Checkpoint: page 15, Figure 2-9 and "Checkpoint rules" section) in another of the plurality of local area network systems, data communicated between one and another terminals of said combination being required to be encrypted;

said central-side encryption unit encrypts the secret concealment terminal data by using each public key assigned to each router, and sends the encrypted secret concealment terminal data to each router (User Guide: page 131, "PGPnet Features" specifically features 1, 2, and 6, "wizard configuration"),

said first router-side decryption unit (Intro: page 6, "How PGP Works" section and Figure 1-4) decrypts the encrypted secret concealment terminal data sent by the central-side encryption unit by using the secret key of the router,

said storage unit (User Guide: page 15, "System Requirements" section) stores the secret concealment terminal data after decryption, and

said router-side encryption unit (User Guide: page 131, "PGPnet Features" specifically features 4, "security associations") encrypts the communication data if the combination of the first source terminal and the first destination terminal is contained in the secret concealment terminal data.

11. As per claim 4, PGP anticipates, the communication network system according to claim 1, wherein said router further comprises:

a second router-side decryption unit for decrypting data sent from a second source terminal in another local area network system to a second destination terminal in the local area network system of the router, and sending the data after decryption to said second destination terminal (User Guide: page 132, "What is PGPnet?", last paragraph).

12. As per claim 5, PGP anticipates, the communication network system according to claim 4, wherein

said management database further stores (Checkpoint: page 15, Figure 2-9 and "Checkpoint rules" section) secret concealment terminal data indicating a combination of one terminal in one of the plurality of local area network systems and another terminal in another of the plurality of local area network systems,

data communicated between one and another terminals of said combination being required to be encrypted,

said central-side encryption unit (User Guide: page 131, "PGPnet Features" specifically features 1, 2, and 6) encrypts said secret concealment terminal data by using each public key assigned to each router, and sends the encrypted secret concealment terminal data to each router,

said first router-side decryption unit (Intro: page 6, "How PGP Works" section and Figure 1-4) decrypts the encrypted secret concealment terminal data sent by the central side encryption unit, by using the secret key of the router,

said storage unit (User Guide: page 15, "System Requirements" section) stores the secret concealment terminal data after decryption, and

said second router-side decryption unit decrypts the communication data if (User Guide: page 132, "What is PGPnet?", last paragraph) the combination of the second source terminal and the second destination terminal is contained in the secret concealment terminal data.

13. As per claim 6, PGP anticipates, the communication network system according to claim 1, wherein

if the common key (User Guide: page 229, definition "session key") stored in the management database is updated, said central-side encryption unit encrypts the updated common key and sends the updated and encrypted common key, and said first router-side decryption unit decrypts the updated and

encrypted common key, and said storage unit substitutes the already stored common key by the updated common key after decryption, for storage.

14. As per claim 7, PGP anticipates, The communication network system according to claim 2, wherein

if the public key stored in the management database is updated (User Guide: page 62, "Updating you key on a certificate server" section), said central-side encryption unit encrypts the updated public key and sends the updated and encrypted public key, and said first router-side decryption unit decrypts the updated and encrypted public key, and said storage unit substitutes the already stored public key by the updated public key after decryption, for storage.

15. As per claim 8, PGP anticipates, the communication network system according to claim 3, wherein

if said secret concealment terminal data stored in the management database is updated (User Guide: page 155, "Modifying a host, subnet, or gateway entry" section), said central-side encryption unit encrypts the updated secret concealment terminal data and sends the updated and encrypted secret concealment terminal data, and said first router-side decryption unit decrypts the updated and encrypted secret concealment terminal data, and said storage unit substitutes the already stored secret concealment terminal data by the updated secret concealment terminal data after decryption, for storage.

16. As per claim 9, PGP anticipates, the communication network system according to claim 5, wherein

if said secret concealment terminal data stored in the management database is updated (User Guide: page 155, "Modifying a host, subnet, or gateway entry" section), said central-side encryption unit encrypts the updated secret concealment terminal data and sends the updated and encrypted secret concealment terminal data, and said first router-side decryption unit decrypts the updated and encrypted secret concealment terminal data, and said storage unit substitutes the already stored secret concealment terminal data by the updated secret concealment terminal data after decryption, for storage.

17. As per claim 10, PGP anticipates, a communication method in a communication network system having a central management device and a plurality of local area network systems, said central management device and said plurality of local area network systems being connected to each other, each of the plurality of local area network systems having a router and a terminal which are connected to each other via a local area network, comprising steps of:

in said central management device,

encrypting at least one common key (User Guide: page 229, definition "session key") stored in a management database in advance by using each public key assigned to each router, each public key being stored in said management database in advance; and

sending the encrypted common key (User Guide: page 229, definition "session key") to each router; and

in said router,

decrypting the encrypted common key sent from the central management device by using a secret key of the router (Intro: page 5, second paragraph and Figure 1-3);

encrypting communication data (Intro: page 6, "How PGP Works" section and Figure 1-4) to be sent from a source terminal in a local area network system of the router to a destination terminal in another local area network system, or communication data to be sent from the router to the central management device by using the common key; and

sending the encrypted communication data to another local area network (User Guide: page 130, "How does a PGP VPN work?" section) or the central management device.

18. As per claim 11, PGP anticipates, a router disposed in each of a plurality of local area network systems which are connected to a central management device, the router being connected via a local area network to a terminal disposed in each of the plurality of local area network systems, the router comprising:

a decryption unit (Intro: page 5, second paragraph and Figure 1-3) for decrypting an encrypted common key sent from said central management device, by using a secret key for said router, said common key being encrypted by using a public key for the router;

a storage unit for storing said common key (User Guide: page 15, "System Requirements" section) after decryption by said decryption unit; and

an encryption unit for encrypting communication data (Intro: page 6, "How PGP Works" section and Figure 1-4) to be sent from a source terminal in a local area network system of said router to a destination terminal in another local area network system, or communication data to be sent from said router to the central management device, by using the common key stored in said storage unit, and sending the encrypted communication data to another local area network or the central management device.

19. As per claim 12, PGP anticipates, a communication method of a router in each of a plurality of local area network systems which are connected to a central management device, said router being connected to a terminal via a local area network, comprising steps of:

decrypting an encrypted common key (Intro: page 5, second paragraph and Figure 1-3) sent from said central management device by using a secret key for said router, said common key being encrypted by using a public key for said router;

storing the common key after decryption in a storage unit (User Guide: page 15, "System Requirements" section) in the router;

encrypting communication data (Intro: page 6, "How PGP Works" section and Figure 1-4) to be sent from a source terminal in a local area network system of the router to a destination terminal (User Guide: page 130, "How does a PGP VPN work?" section) in another local area network system, or communication

data to be sent from the router to the central management device, by using the common key stored in the storage unit; and

 sending the encrypted communication data to another local area network or to the central management device (User Guide: page 130, "How does a PGP VPN work?" section).

20. As per claim 13, PGP anticipates, a program product executed by a router disposed in each of a plurality of local area network systems which are connected to a central management device, the router being connected via a local area network to a terminal disposed in each of the plurality of local area network systems, said program product comprising steps of:

 decrypting an encrypted common key (Intro: page 5, second paragraph and Figure 1-3) sent from the central management device by using a secret key of the router, said common key being encrypted by using a public key of the router;

 storing said common key after decryption in a storage unit (Intro: page 5, second paragraph and Figure 1-3) of the router;

 encrypting communication (Intro: page 6, "How PGP Works" section and Figure 1-4) data to be sent from a source terminal in a local area network system of the router to a destination terminal (User Guide: page 130, "How does a PGP VPN work?" section) in another local area network system, or communication data to be sent from the router to the central management device, by using the common key stored in the storage unit ; and

sending the encrypted communication data (User Guide: page 130, "How does a PGP VPN work?" section) to another local area network or to the central management device.

21. As per claim 14, PGP anticipates, a central management device connected to a plurality of local area network systems each having a router and a terminal which are connected to each other through a local area network, the central management device comprising:

a management database (User Guide: page 230, definition "trusted introducer") for storing at least one common key, each public key assigned to each router and a public key assigned to said central management device (User Guide: page 228, definition "public keyring"), said at least one common key (User Guide: page 229, definition "session key") being used by each router to encrypt communication data to be communicated between a terminal of a local area network system and a terminal of another local area network system, or between each router and the central management device (User Guide: page 130, "How does a PGP VPN work?" section); and

an encryption unit (Intro: page 5, second paragraph and Figure 1-3) for encrypting the common key by using each public key assigned to each router, and sending the encrypted common key to each router.

22. As per claim 15, PGP anticipates, a management method of a central management device connected to a plurality of local area network systems each having

Art Unit: 2136

a router and a terminal which are connected to each other through a local area network, the management method comprising steps of:

storing (User Guide: page 15, "System Requirements" section) in a management database (User Guide: page 228, definition "public keyring") and managing at least one common key, each public key assigned to each router and a public key assigned to said central management device, said at least one common key being used by each router to encrypt communication data (User Guide: page 229, definition "session key") to be communicated between a terminal in a local area network system and a terminal in another local area network system, or between a router and the central management device (User Guide: page 130, "How does a PGP VPN work?" section);

encrypting the common key (Intro: page 6, "How PGP Works" section and Figure 1-4) by using each public key assigned to each router; and

sending the encrypted common key (Intro: page 6, "How PGP Works" section and Figure 1-4) to each router.

23. As per claim 16, PGP anticipates, a program product executed by a computer installed in a central management device connected to a plurality of local area network system each having a router and a terminal which are connected to each other through a local area network, said program product comprising steps of:

storing (User Guide: page 15, "System Requirements" section) in a management database (User Guide: page 228, definition "public keyring") and managing at least one common key, each public key assigned to each router and

Art Unit: 2136

a public key assigned to said central management device, said at least one common key (User Guide: page 229, definition "session key") being used by each router to encrypt communication data to be communicated between a terminal in a local area network system and a terminal in another local area network system, or between a router and the central management device (User Guide: page 130, "How does a PGP VPN work?" section);

encrypting the common key by (Intro: page 6, "How PGP Works" section and Figure 1-4) using each public key assigned to each router; and

sending the encrypted common key (Intro: page 6, "How PGP Works" section and Figure 1-4) to each router (User Guide: page 229, definition "session key").

Conclusion

24. A concise list of all citation used from the PGP documentation includes:
25. (User Guide: page 228, definition "public keyring")
26. (User Guide: page 229, definition "session key")
27. (User Guide: page 230, definition "trusted introducer")
28. (Intro: page 5, second paragraph and Figure 1-3)
29. (Intro: page 6, "How PGP Works" section and Figure 1-4)
30. (User Guide: page 15, "System Requirements" section)
31. (Checkpoint: page 15, Figure 2-9 and "Checkpoint rules" section)
32. (User Guide: page 131, "PGPnet Features" specifically features 1, 2, and 6)

Art Unit: 2136

33. (User Guide: page 131, "PGPnet Features" specifically features 4, "security associations")
34. (User Guide: page 132, "What is PGPnet?", last paragraph)
35. (User Guide: page 62, "Updating you key on a certificate server" section)
36. (User Guide: page 155, "Modifying a host, subnet, or gateway entry" section)
37. (User Guide: page 130, "How does a PGP VPN work?" section)
38. Research, done while executing an examination of the present application, used but not relied upon includes:
 39. PGP Corporation, "PGP History", Most recent update 2005, www.pgp.com/company/history.html
 40. Research done while executing and examination of the present application used but not relied upon includes:
 41. Microsoft Technical Resources, "Virtual Private Networking: Frequently Asked Questions", 21 July 2003, www.microsoft.com
 42. AT&T WorldNet Support, "AT&T WorldNet Virtual Private Network Service: User Guide", version 2.7, 18 August 1999
 43. Indiana University: University Information Technology Services, "IU VPN for Windows NT 4.0", 12 March 2003, support.iupui.edu/vpn/winnt/home.html
 44. Paul Ferguson, "What is a VPN?", April 1998
 45. Douglas Maughan, Mark Schertler, National Security Agency, "Internet Security Association and Key Management Protocol (ISAKMP)" (a.k.a. IPsec White Paper), 21 February 1996

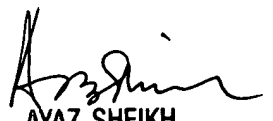
46. RSA Laboratories, "Crypto FAQ", Chapter 3, Section 3.6, "What is Diffie-Hellman?"
47. Greg Marcotte, Network World, "Protocols serve up VPN security", 31 May 1999
48. Adam Back, "PGP timeline and brief history", cypherspace.org/adam/timeline/
49. United States Patents numbered 6,895,501 and 6,662,299.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nathan D. Hast whose telephone number is (571) 272-6558. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nathan D. Hast
Examiner
Art Unit 2136


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100